International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-11 Issue-6, May 2022

Detection and Investigation of DDoS Attacks in Network Traffic using Machine Learning Algorithms

Biswajit Mondal, Chandan Koner, Monalisa Chakraborty, Subir Gupta

Abstract*: The Internet of Things (IoT) represents the start of a new age in information technology (IoT). Objects (things) such as smart TVs, telephones, and smartwatches may now connect to the Internet. New services and software improve many consumers' lives. Online lessons based on COVID-9 are also included in child education devices. Multiple device integration is becoming more widespread as the Internet of Things (IoT) grows in popularity. While IoT devices offer tremendous advantages, they may also create network disruptions. This article summarises current DDoS intrusion detection research utilizing machine learning methods. This study examines the detection performance of DDoS attacks utilizing WEKA tools using the most recent NSL KDD datasets. Logistic Regression (LR), Naive Bayes (NB), SVM, K-NN, Decision Tree (DT), and Random Forest (RF) are examples of Machine Learning algorithms. Using K-Nearest Neighbors in the presented assessment (K-NN), accuracy was attained. Finally, future research questions are addressed.

***Keywords*: DDoS Attacks; Internet Of Things; Machine Learning**

I. INTRODUCTION

As computing networks, particularly the internet, grow in size, network attacks are becoming increasingly widespread. The Wannacryransomware infection has caused the internet to be inaccessible in 156 nations. Kaspersky Lab identified botnet-assisted attacks on assets in 69 different countries during the fourth quarter. Furthermore, the botnet-based DDoS attack that lasted the longest happened in the previous quarter (15.5 days, 371 hours)[1][2]. Cybercriminals continually develop tiered distributed denial of service (DDoS) techniques that attack the OSI network and application layers. These attacks employed faked IP addresses to fool source detection and launch a large-scale wave of attacks[3][4]. These attacks are massive, using a considerable percentage of the network's spectrum during peak hours and interfering with the transmission of legitimate packets. Ironically, governments, banks, militaries, and defense forces have all been attacked. DDoS attacks against well-known websites such as Facebook, Twitter, and Wikileaks have resulted in financial losses, service degradation, and lack of access. Services might be swamped or crashed in one of two ways. In floods, the target system becomes excessively sluggish, eventually failing to respond at all. DDOS is a more severe and difficult-to-detect distributed denial-of-service assault. A denial of service attack is referred to as a "Distributed Denial of Service." This article describes a machine-learning technique for detecting and analyzing attacks such as Smurf, UDP flooding, and HTTP flooding[5]. Because there are no particular data sets containing contemporary DDoS assaults on several levels, such as SI-DDoS and HTTP flood, this study was done on a new dataset containing new types of DDoS attacks produced expressly for this purpose. According to the findings of comparing the various classification algorithms, MPL has the most remarkable accuracy rate[6].

Manuscript received on 02 April 2022.
Revised Manuscript received on 05 April 2022.
Manuscript published on 30 May 2022.
* Correspondence Author
Mr. Biswajit Mondal, Department of Computer Science and Engineering, Dr. B. C. Roy Engineering College, Durgapur, West Bengal 713206, India. Email: biswa.mondal@gmail.com
Dr. Chandan Koner, Department of Computer Science and Engineering, Dr. B. C. Roy Engineering College, Durgapur, West Bengal 713206, India. Email: chandan.koner@bcrec.ac.in
Miss. Monalisa Chakraborty, Department of Computer Science and Engineering, Dr. B. C. Roy Engineering College, Durgapur, West Bengal 713206, India.. Email: chakraborty.monalisa6@gmail.com
Dr. Subir Gupta*, Department of Computer Science and Engineering, Dr. B. C. Roy Engineering College, Durgapur, West Bengal 713206, India. Email: subir2276@gmail.com

II. LITERATURE REVIEW

DDoS attacks may be detected and blocked using an application-layer method. SVM was used by them (Support Vector Machine). As a result, it's not clear how accurate the approach is in detecting DDoS attacks at the application layer[7][8][9]. The Ploy Kernel and Sequential Minima Optimization (SMO) could not foresee a distributed denial of service attack. Two sets of data were used in this study. The proposed method was shown to be extremely accurate with a low percentage of false alarms. Another group of academics has developed a method for detecting Denial-of-Service attacks using an artificial neural network (ANN). The technique was tested using the CICIDS2017 dataset[10]. An extra seven layers are proposed by Yadigar Imamverdiyev to cover the machine's input and output levels in a restricted Boltzmann device of the Gaussian-Beroni type. In terms of danger detection, only a few researchers have examined the efficacy of several machine learning methods. They found a number of characteristics that may be tweaked to further improve the algorithms' precision. Several scientists have also proposed a machine learning-based approach for identifying distributed denial of service (DDoS) attacks[11][12]. The suggested system's accuracy and warning categories were evaluated using a variety of machine learning methods.

Several data mining approaches were also tested for their potential to identify DDOS attacks. Fuzzy c-means has been shown to be the most effective technique. researchers discovered a solution to reduce SYN-flooding in software-defined networking network interfaces (SDN)[13]. In order to accomplish this, they turned to machine learning (ML). Using the KNN classification approach, the important features of port numbers per IP address, such as entropy, are analysed. Even though the CatBoost technique is more precise, it is more time-consuming to train. It was possible to detect DDoS assaults using SVM and community clustering. Diversity and normalised entropy are two characteristics that might be used to make a decision. For identifying DDoS in IoT systems, DDAML transcends current algorithms and provides three techniques using SVM, LPA, QDA, and KNN. Naive Bayes and random forest classifiers were used in the development of a DDoS detection technique. Some propose a hybrid DDoS detection system that uses both known signatures and anomaly-based detection approaches to identify assaults. DDoS attacks on SDNs may now be detected using an approach developed by Gaganjot Kaur and others. The KDDCUP99 dataset is implemented using SVMs and ANNs in the system. The system outperforms KNN in terms of performance[14].

III. BACKGROUND KNOWLEDGE AND DATASET

DDos attack in different OSI layer displays in the Table 1.

Table 1: Types of DDo Sattck

OSI Layer	Possible DOS/DDOS attack
Application	HTTP POST and GET
Presentation	Malformed SSL requests
Session	Telnet DDOS
Transport	Smurf , SYN Flood
Network	ICMP Flooding attack
Data Link	MAC Flooding attack
Physical	Malfunction of physical assets

A. HTTP flood attack (GET & POST)

To overwhelm a web server or application, a real HTTP GET or POST request is made. A botnet zombie army, or a network of infected workstations linked together, is used in volumetric HTTP flood assaults. HTTP floods are sophisticated Layer 7 attacks that need less bandwidth. It is necessary to understand the target site or application. As a result, preventing HTTP floods is tough. A web browser makes GET or POST requests to a programme or server. For example, GET and POST requests, for example, return static images and dynamic data, respectively. Imperva blocks DDoS attacks from 180,000 botnet IPs. As a result, in order for a server or application to function properly, it must provide the greatest number of resources for each request. Attackers intend to overload servers or apps. As a consequence, POST queries are often the least resource-intensive. In a botnet, HTTP GET attacks are easy to create and scale.

B. Malformed SSL requests Attack

SSL encryption is used to secure data in many network communication protocols. Threats increase as more transactions and services using SSL. SSL services are now vulnerable to DDoS attacks that use flood and TCP connection-based state depletion. Unwanted data is delivered to the SSL server, causing connection problems for genuine users or causing the SSL handshake protocol to fail. Many DDoS assaults are directed at the SSL handshake. The Pushdo botnet does this by sending spam to an SSL server. Using the SSL protocol to treat trash as a genuine server handshake, Firewalls do not detect invalid SSL handshake packets. Before requesting re-encryption, the THC-SSL-DOS program performs a regular SSL handshake. It wants more renegotiations and so forth. If the server has blocked SSL renegotiation, the software ends the SSL connection and initiates a new one. Due to resource depletion, genuine users are unable to access services. Others may target SSL negotiation to overwhelm servers and prevent service delivery.

C. Telnet DDOS attack

We had to configure a large number of switches and routers at the same time. Specifically, we must configure or troubleshoot many devices at the same time almost every time. Of course, we don't want to reattach the console cable to every other switch just to show how it works. We want to be able to connect to all devices at the same time and then use different command prompts for each. As a result, we can debug and configure more quickly without having to swap the console wires. We may also compare different configurations by opening two command prompts next to each other. To avoid the attacks outlined below, use SSH instead. For example, more and more modern PCs do not even support telnet (for example, F5 devices).

D. Telnet Attacks

Telnet assaults are divided into many types: Telnet communication sniffing, Telnet brute force attacks, etc.

a) Telnet Communication Sniffing

Above all, telnet is unencrypted. The remote device transmits plain text messages to the networking device chosen. Frame sniffing is now possible with our command. The attacker can see our activity on the device and the password we used to get in and set it up. Telnet is no longer used outside of labs since it is easier to configure than SSH. SSH is now used in all other instances. While using SSH instead of telnet solves the most critical security issue, there are other ways to abuse telnet.

b) Telnet Brute Force Attack

An attacker can use Telnet to get remote access to a Cisco physical network or other vendors' networks. We are still not safe if we configure a password for the leased lines and need password authentication to access the switch. This VTY password only on socket lines protects the control from unauthorized access.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

However, it does not prevent unauthorized access to the VTY connections. There are numerous tools on the switch's VTY lines that can do brute-force password cracking.

E. SYN Flood attack

A SYN flood (half-open assault) is a type of DDoS attack that utilises all server resources that are available. An attacker can overflow all accessible ports on a given server by sending SYN packets indefinitely, forcing it to respond slowly or not at all to legitimate traffic. SYN flood attacks take advantage of the TCP handshake mechanism. Normally. A malicious person can use an SYN flood attack to stop service to a target device or service, but this attack uses a lot less bandwidth than a typical DDoSattack.These attacks do not need to fill up the target's network. Instead, they need to be bigger than their target's operating system's "backlog."An attacker must know the amount of the backlog and how long each connection will be open before clocking out in order to plan a denial-of-service assault.

F. Smurf attack

A distributed denial of service attack at the network layer is called a "Smurf." It is spyware that allows it to function. Ping floods and smurf attacks are similar in that they both send out a high number of ICMP Echo request packets. A Smurf is an amplification attack vector that uses broadcast network features instead of a traditional ping flood. In most cases, host A will send a ping to host B, which will get an automatic response. Response time is required to compute the virtual distance between two hosts. Each server in an IP broadcast network replies to a ping request. Smurf attack perpetrators utilize this feature to enhance attack traffic.

G. ICMP Flooding attack

An ICMP flood DDoS attack, also known as a Ping flood attack, attempts to overwhelm a targeted device with multiple ICMP echo-requests (pings). Typically, ICMP echo-request and echo-reply messages are used to ping a network device in order to examine its health and connection, as well as the sender-device relationship. The network is forced to respond after being bombarded with request packets from the target. Normal traffic is then unable to reach its destination. Some ICMP request attacks make use of specialised tools or code, such as hping and scapy. DDoS assaults are attacks that come from a large number of devices. Both incoming and outgoing network channels are full of this type of DDoS attack. This results in a loss of service.

H. MAC Flooding attack

MAC flooding is a security risk to network switches. The majority of controllers keep MAC tables. The MAC address of each switch port is mentioned here. Controllers can use this table to convey data to ports. Switches transfer data to individual hosts, whereas hubs broadcast data to the whole network. MAC tables can be helpful, too. To eradicate the MAC Table, MAC flooding sends hundreds of Ethernet packets at once. The sender addresses on the switch differ. The opponent wishes to obtain the MAC RAM. The MAC addresses of valid users will be erased. As a result, the controller is unable to deliver data. As a result, all ports will be inundated. The MAC Address Table is filled. It activates the switch and turns it into a network hub. It will transmit data to all available ports. Investigate the attacker's MAC flooding advantages. Because the attacker is in the network, he receives the victim's data packets. They were keeping a victim's PC and other systems secure. A packet analyzer is a standard piece of equipment. After a successful MAC Flood attack, ARP spoofing can be employed. As a result of MAC flooding, the attacker now has access to confidential data.

IV. MACHINE LEARNING METHODS

A. KNN

The K-Nearest Neighbor method is a basic supervised learning technique. The K-NN technique assumes a high degree of similarity between incoming instances/data and current cases and assigns them to the most related category feasible. The K-NN approach compares all of the available data against data that has already been stored. Using the K-NN technique, new data may be quickly categorised into the most relevant category. The K-NN technique may be used to solve issues in both regression and classification. True, the K-NN technique is not a parametric method, which means it does not make any assumptions about the data. It is also called the "lazy learner" method since it does not instantly learn from a training set but instead retains the information and then uses it to categorize the results. The KNN algorithm saves the data and puts it into a category that is the same as the data that came in during the training phase[15].

B. SVM

SVM is a supervised learning technique often used to solve classification and regression issues. However, it is widely used in machine learning for categorization, which explains its popularity. As a result, the SVM method seeks to find the optimal line or decision boundary that divides n-dimensional space into classes. New data points may be classified as rapidly as feasible in the future. A hyperplane represents the limit of the best possible option. An SVM is used to pick the hyperplane's extreme points or vectors[16][17].

C. Naïve Bayes(NB)

The Naive Bayes method is used for categorisation and is based on Bayes' theorem. In text classification, a high-dimensional training dataset is typically used. One of the most effective and fundamental classification methods for developing rapid machine learning models that can give quick predictions is the Nave Bayes Classifier. The probability of an object is used to anticipate the classifier's output[18]. The Naive Bayes Algorithm is used in spam filters, sentiment analysis, and article categorization.

D. Decision Tree(DT)

A decision tree can be used to solve classification and regression issues. Internal nodes for dataset properties, branches for decision rules, and leaf nodes at the end. This is a decision tree with two nodes. Decision nodes generate leaf nodes, which have no further branching. Based on the dataset's attributes, It generates a graph of all possible solutions to a problem.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

It's called a "decision tree" because, like a tree, it grows from the ground up. We use the CART algorithm (Classification and Regression Tree) to create a tree. A decision tree divides itself into subtrees based on the answer to a query. a) Because they mimic human decision-making, decision trees are intuitive. The logic of the decision tree is simple by definition[19][20].

E. Random Forest (RF)

Random Forest is a popular supervised learning technique. They are used in machine learning classification and regression. It employs ensemble learning, which combines many classifiers to solve a complex problem and improve model performance. A Random Forest employs several decision trees on distinct subsets of the input dataset to improve forecasting accuracy. Instead of relying on a single decision tree, the random forest considers each tree's predictions and predicts the ultimate output based on the majority vote. The presence of additional trees in the forest enhances accuracy while reducing overfitting. Because the random forest employs many trees to forecast the class of the dataset, some decision trees may be correct while others may be incorrect. However, the trees anticipate appropriately as a group[21][6].

F. Logistic Regression (LR)

Regression is a popular Supervised Learning method. In this case, the dependent variable is categorical. Statistics forecasts the outcomes of dependent variables. As a result, the product must be definite. Yes, or No, 0 or 1, true or false, but always between 0 and 1. Logistic Regression is used in the same way that Linear Regression is. It has the potential to be utilized for Regression or classification. We use an "S" shaped logistic function instead of a regression line (0 or 1). The logistic function's curve represents the possibility of anything, such as malignant cells or a fat animal. This machine learning approach performs admirably on both continuous and discrete datasets. You may categorize data and discover the most efficient classification factors using Logistic Regression. The sigmoid function is used to calculate probability. It modifies any actual number ranging from 0 to 1. The logistic regression outcome must be 0 and 1, resulting in an "S" curve. The sigmoid function is represented as an S-shaped curve. Use logistic Regression to compute the likelihood of 0 or 1. According to the logistic regression equation, values above and below the cutoff tend to be 1[22][23][2].

V. MEASUREMENT MATRICS

This section provides an overview of our mathematical performance measurements. Parameters are used to compute all values. The causes are detailed in Table 2.

Table 2: Notation vs Arguents name

Notation	Arguents name
Tp	True Positive
Tn	True Negative
Fp	False Positive
Fn	False Positive

Using all of the information, we can compute the accuracy score, precision score, recall score, and F1 score. Training time is another important component evaluated for performance measures in this study. All four (excluding training time) have the following mathematical expressions:

$$AccuracyScore = (Tn + Tp)/(Tn + Fp + Tp + Fn)$$
$$Precision = Tp/(Tp + Fp)$$
$$Recall = Tp/(Tp + Fn)$$
$$F1\ Score = 2 * (Recall * Precision)/(Recall + Precision)$$

Training Time: It is time for a newly created model to be trained using some ML Algorithm.

VI. DATASET

Here Figure 1 shows the dataset collection methodology. We collected data using the "NSL KDD" data collection, which uses publicly available APIs. We reused and aggregated the data from the previous stage during this inquiry. In this respect, data accumulation refers to storing and retaining data counts, linking storage types such as illuminating files to more fundamental accumulating types such as records. When a third party acquires information about a transaction, this is referred to as "pre-dealing knowledge." Purification, extraction, and data fitting are the three phases in data pre-dealing. This is because data cleaning will hunt for flaws in the dataset that might impact the outputs of the provident model. Include extraction while talking about a never-ending Brobdingnagian data approach. To summarise, information fitting is the process of fitting a model to data and then dividing the precision of the fit by two to arrive at the result. The word "illumination dataset" refers to a vast amount of data that has been collected and stored in a specific location.

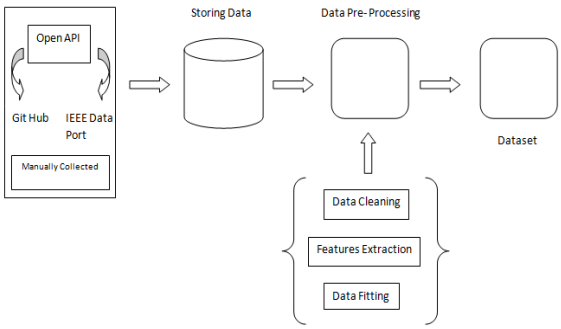

Figure 1: Dataset Collection

VII. RESULT ANALYSIS

Each of the six Mchine Learning examinations has a different cutoff score that must be achieved.

Accuracy	Precision	Recall	F1	CT
0.97	0.98	0.97	1	4.53
0.44	0.65	0.53	0.4	1.3
0.85	0.84	0.86	0.8	6.29
0.97	0.98	0.98	1	2.5
0.98	0.98	0.98	1	3.53
0.98	0.98	0.98	1	74.2

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

shows the cutoff criteria for accuracy, precision, recall, F1 Score, calculation time, and the recall and calculation time cutoff limitations. The K-NN, DT, and RF perform exceedingly well in the most critical performance matrix, the F1 Score, as shown in

Accuracy	Precision	Recall	F1	CT
0.97	0.98	0.97	1	4.53
0.44	0.65	0.53	0.4	1.3
0.85	0.84	0.86	0.8	6.29
0.97	0.98	0.98	1	2.5
0.98	0.98	0.98	1	3.53
0.98	0.98	0.98	1	74.2

, with values averaging 0.98. Without a doubt, the F1 Score is the most visible. In the case of a tie, the calculation time parameter is utilized. In this assessment, the K-Nearest Neighbors (K-NN) method surpassed the decision tree (DT) and the RandomForest (RF) in terms of computing time. The K Nearest Neighbors (K-NN) technique, which has the highest display in Distributed Denial-of-Service (DDoS) assaults disclosure for mark datasets, has been permanently shut down due to a cosmically monstrous communication. Because this study used only one dataset, "NSL KDD," the results of a larger dataset may differ. We think reinforcement learning for DDoS attack detection can give great precision when dealing with real-time challenges. Finally, we are pleased with the accuracy of 0.99 percent.

Table 3: Result analysis of all methods.

ML Algo	Accuracy	Precision	Recall	F1	CT
LR	0.97	0.98	0.97	1	4.53
NB	0.44	0.65	0.53	0.4	1.3
SVM	0.85	0.84	0.86	0.8	6.29
KNN	0.97	0.98	0.98	1	2.5
DT	0.98	0.98	0.98	1	3.53
RF	0.98	0.98	0.98	1	74.2

VIII. CHALLENGES AND FUTURE WORK

The Internet of Things is characterized by limited memory and computer capability andmany standards and protocols. The identification and mitigation of anomalies using IDS have become increasingly complex. Despite much research, fundamental difficulties in IoT anomaly detection remain unresolved. Examples:

1. There are no publicly available datasets of IoT network traffic. Because real-world networks are uncertain, testing and verifying anomaly-avoiding algorithms is difficult. Strategies for anomaly mitigation will be studied and validated.
2. There are no industry-standard IoT authentication apps. Validating implemented structures ensures that they are built correctly. Simulations and testing are used to assess it. Most IDS structures in the IoT are currently not analyzed due to a lack of standard authentication apps. Reliable authentication is required for duplication, reproducibility, and research continuation.
3. The CICDoS2019 dataset uses supervised and unsupervised machine learning techniques like RNN and CNN.
4. Real-time packets can be collected and tested against the training dataset. The data may be separated and compared to classifier performance using fold cross authentication.

IX. CONCLUSION

According to this paper, DDoS assaults cause significant disruption in many aspects of our lives, including education. As a result, to reduce the number of assaults in diverse industrial settings, an effective intrusion detection system must be developed. The NSL KDD dataset, a current and substantial cybersecurity dataset, was used in this work. The study also looked into machine learning methods. Logistic Regression, Nave Bayes, Super Vector Machine, K Nearest Neighbors, Decision Tree, and Random Forest were among them. Logistic Regression, Nave Bayes, and Super Vector Machines were the most researched algorithms (RF). Accuracy and precision, recall, F1 Score, and computation time were the assessment criteria used. The experiment shows that using K-Nearest Neighbors (K-NN) algorithms yields 98 percent accuracy, the highest level currently achievable. Final results indicates that K-NN, DT, and RF perform exceptionally well in the most critical performance matrix (F1 Score), with an average value of 0.98. The F1 Score is, without a doubt, the most discussed. The computation time parameter determines the winner if the game is tied. In this study, the K-Nearest Neighbors (K-NN) technique outperformed both the decision tree and the Random Forest (RF) approaches in terms of computation time. The results reveal that machine learning comes effectively detect attack traffic. Our efforts are designed to supplement existing studies in this field. The experiments indicate that using the K Nearest Neighbors feature selection strategies improves the accuracy of machine learning systems in detecting fraudulent traffic. Because this study employs a real-world scenario, it has the potential to be applied to several Internet of Things applications. Final thoughts on network anomaly mitigation strategies for IoT security. In this section, we will look at their potential.

REFERENCE

1. V. Kanimozhi and T. P. Jacob, “Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing,” ICT Express, vol. 7, no. 3, pp. 366–370, 2020, doi: 10.1016/j.icte.2020.12.004.
2. G. Kaur, V. Saxena, and J. P. Gupta, “Detection of TCP targeted high bandwidth attacks using self-similarity,” J. King Saud Univ. - Comput. Inf. Sci., vol. 32, no. 1, pp. 35–49, Jan. 2020, doi: 10.1016/j.jksuci.2017.05.004.
3. C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, “Ransomware: Recent advances, analysis, challenges and future research directions,” Comput. Secur., vol. 111, p. 102490, 2021, doi: 10.1016/j.cose.2021.102490.
4. S. Ibrahim, “Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals,” Int. J. Law, Crime Justice, vol. 47, pp. 44–57, Dec. 2016, doi: 10.1016/j.ijlcj.2016.07.002.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

5. M. Alkasassbeh, G. Al-Naymat, A. B.A, and M. Almseidin, "Detecting Distributed Denial of Service Attacks Using Data Mining Techniques," Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 1, pp. 436–445, 2016, doi: 10.14569/ijacsa.2016.070159.
6. S. Gupta, J. Sarkar, A. Banerjee, N. R. Bandyopadhyay, and S. Ganguly, "Grain Boundary Detection and Phase Segmentation of SEM Ferrite–Pearlite Microstructure Using SLIC and Skeletonization," J. Inst. Eng. Ser. D, vol. 100, no. 2, pp. 203–210, Oct. 2019, doi: 10.1007/s40033-019-00194-1.
7. S. K. Singh and A. K. Gupta, "Application of support vector regression in predicting thickness strains in hydro-mechanical deep drawing and comparison with ANN and FEM," CIRP J. Manuf. Sci. Technol., vol. 3, no. 1, pp. 66–72, 2010, doi: 10.1016/j.cirpj.2010.07.005.
8. T. Subbulakshmi, K. Balakrishnan, S. M. Shalinie, D. Anandkumar, V. Ganapathisubramanian, and K. Kannathal, "Detection of DDoS attacks using Enhanced Support Vector Machines with real time generated dataset," 3rd Int. Conf. Adv. Comput. ICoAC 2011, pp. 17–22, 2011, doi: 10.1109/ICoAC.2011.6165212.
9. H. Waguih, "A Data Mining Approach for the Detection of Denial of Service Attack," IAES Int. J. Artif. Intell., vol. 2, no. 2, 2013, doi: 10.11591/ij-ai.v2i2.1937.
10. J. KaurBains, K. Kumar Kaki, and K. Sharma, "Intrusion Detection System with Multi Layer using Bayesian Networks," Int. J. Comput. Appl., vol. 67, no. 5, pp. 1–4, 2013, doi: 10.5120/11388-6680.
11. "Erratum regarding missing Declaration of Competing Interest statements in previously published articles (Journal of King Saud University - Computer and Information Sciences, (S1319157818300545), (10.1016/j.jksuci.2018.04.001))," Journal of King Saud University - Computer and Information Sciences, vol. 32, no. 10. King Saud bin Abdulaziz University, pp. 1206–1207, Dec. 01, 2020, doi: 10.1016/j.jksuci.2020.10.026.
12. A. Bivens, C. Palagiri, R. Smith, B. Szymanski, and M. Embrechts, "Network-based intrusion detection using neural networks," Intell. Eng. Syst. Through Artif. Neural Networks, vol. 12, pp. 579–584, 2002.
13. S. Seufert and D. O'brien, "Machine learning for automatic defence against distributed denial of service attacks," in IEEE International Conference on Communications, 2007, pp. 1217–1222, doi: 10.1109/ICC.2007.206.
14. S. T, P. P, P. C, M. M, A. A. J, and M. G, "a Unified Approach for Detection and Prevention of Ddos Attacks Using Enhanced Support Vector Machines and Filtering Mechanisms," ICTACT J. Commun. Technol., vol. 04, no. 02, pp. 737–743, 2013, doi: 10.21917/ijct.2013.0105.
15. J. Wang and M. Wang, "Review of the emotional feature extraction and classification using EEG signals," Cogn. Robot., vol. 1, no. December 2020, pp. 29–40, 2021, doi: 10.1016/j.cogr.2021.04.001.
16. G. G. Sundarkumar and V. Ravi, "A novel hybrid undersampling method for mining unbalanced datasets in banking and insurance," Eng. Appl. Artif. Intell., vol. 37, pp. 368–377, 2015, doi: 10.1016/j.engappai.2014.09.019.
17. B. T. Pham and I. Prakash, "Evaluation and comparison of LogitBoost Ensemble, Fisher's Linear Discriminant Analysis, logistic regression and support vector machines methods for landslide susceptibility mapping," Geocarto Int., vol. 34, no. 3, pp. 316–333, 2019, doi: 10.1080/10106049.2017.1404141.
18. O. S. Al-Kadi, "Supervised texture segmentation: A comparative study," 2011, doi: 10.1109/AEECT.2011.6132529.
19. Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Machine learning-based IoT-botnet attack detection with sequential architecture," Sensors (Switzerland), vol. 20, no. 16, pp. 1–15, Aug. 2020, doi: 10.3390/s20164372.
20. S. Gupta, "Chan-vese segmentation of SEM ferrite-pearlite microstructure and prediction of grain boundary," Int. J. Innov. Technol. Explor. Eng., vol. 8, no. 10, pp. 1495–1498, 2019, doi: 10.35940/ijitee.A1024.0881019.
21. S. Gupta et al., "Modelling the steel microstructure knowledge for in-silico recognition of phases using machine learning," Mater. Chem. Phys., vol. 252, no. May, p. 123286, Sep. 2020, doi: 10.1016/j.matchemphys.2020.123286.
22. I. H. Sarker, "CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks," Internet of Things, vol. 14, p. 100393, Jun. 2021, doi: 10.1016/j.iot.2021.100393.
23. S. Panda, A. K. Ghosh, A. Das, U. Dey, and S. Gupta, "Machine Learning-based Linear regression way to deal with making data science model for checking the sufficiency of night curfew in Maharashtra , India," Int. J. Eng. Appl. Phys., vol. 1, no. 2, pp. 168–173, 2021.

AUTHORS PROFILE

Mr. Mondal is working as as an Assistant Professor in the Department of CSE, at Dr. B. C Roy Engineering College, Durgapur, West Bengal, India .He has completed M.Tech from University of Calcutta in C.S.E and presently pursuing his P.hD .

Dr. Chandan Koner did his Ph .D. in CSE in 2012 from Jadavpur University. Now he is Professor and HOD of the CSE Department of Dr. B. C. Roy Engineering College, Durgapur. He has more than seventeen years of teaching experience in different engineering colleges. Dr. Koner is a Fellow of IETE, IE(I), South Asian Chamber of Scientific Research & Development, Nikhil Bharat Shiksha Parisad, Senior Member of ORSI, Member of CSI, ISTE, ISCA, IACSIT, Singapore, UACEE, Australia and IRSS, Canada. He is Member of Executive Committee of The Institution of Engineers (India), Durgapur Local Centre.

Miss Monalisa Chakrborty is working as an Assistant Professor in the Department of CSE, at Dr. B. C Roy Engineering College, Durgapur, West Bengal, India. Miss Chakrborty is an M.E in CSE from B.U., WB, India

Dr. Subir Gupta is working as an Assistant Professor in the Department of CSE, at Dr. B. C Roy Engineering College, Durgapur, West Bengal, India. Dr. Gupta Ph.D. in Engineering from IIEST, Shibpur, Howrah, WB, India.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)